

### REMARKS

Claims 19-22, 26, 27, 29 and 31-47 are pending in the application and claims 19-22, 27, 29, 31, 32, 34-39, 41, 42, 44, 45 and 47 stand rejected.

#### Objections to the claims

Claims 19-22, 26, 27, 29 and 31-47 are objected to for reciting the limitation "operable." These claims have been amended to now recite "configured" instead, pursuant to the Examiner's suggestion, and Applicants submit that this objection is now moot.

#### Rejection under 35 U.S.C §103

Claims 19-22, 27, 29, 31, 32, 35-39, 41, 42, 44, 45 and 47 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Pat. No. 6,092,147 to Levy et al. in view of U.S. Pat. No. 5,724,425 to Chang et al. In particular, with respect to claims 19-21 and 29, the Examiner finds that Levy discloses all claimed limitations with the sole exception that, although it is mentioned that the bytecode verification in the bytecode authenticator uses a suitable cryptographic computation such as a digital signature using an asymmetric cryptographic algorithm, the details of such cryptographic computation are not explicitly disclosed. The Examiner further finds that Chang discloses the use of a passport (which the Examiner likens to a trusted module) in a scheme for protecting source code, and opines that it would have been obvious to modify the teachings of Levy with those of Chang because it would allow including a valid passport as disclosed by Chang in the tamper-resistant package of Levy in order to provide the basis of a trust model and allow computer users to identify and determined the genuineness of a software product based on the information contained in its passport. Applicants respectfully disagree.

At the outset, Applicants note that the Examiner has misinterpreted the disclosure of Levy. For instance, Levy does not disclose a trusted module that is resistant to *internal* tampering. The portion of Levy at col. 7 ll. 46-55 cited by the Examiner teaches that:

As described above, to further ensure the security of the VM and the close association between the loader, the back end verifier and the interpreter, all of the functional units may be located within the single physically tamper-resistant package 66. The tamper-resistant package may be a plastic encased single semiconductor die, for portable secure products such as a smart card, or may be a mechanically sealed casing for multiple-chip products, such as PIN-pads, or set-top boxes. Now, the bytecodes store 80 will be described. [emphasis added]

As the above paragraph makes clear, Levy only contemplates circuit that is resistant to *external* tampering, that is, a brute force attempt to *physically* alter the circuit. As those skilled in the art will immediately recognize, providing a mechanically sealed casing does not protect a circuit from internal tampering, which is a process accomplished through malicious software. As such, illustrative, non-limiting examples of methods for rendering the claimed trusted module resistant to internal tampering that are described in the specification include, *inter alia*, storing a profile within the trusted module, storing logs within the trusted module, using the trusted module not only to protect keys but also to provide the encryption and decryption functionality (which approach is more secure than using the main CPU), using a specialized authorization code to trigger the trusted module to perform the decryption (which uses a different key), using the trusted module as part of the operating system, etc. Applicants submit that there is nothing akin to these, or any other, methods disclosed by Levy that would in fact render the physically tamper-resistant package 66 of Levy resistant to internal tampering, and should the Examiner insist upon this point of view, Applicants respectfully request her to clearly and specifically point out where Levy discloses this feature in accordance with 37 C.F.R. 1.104(c)2.

Applicants also respectfully disagree that the software passport of Chang reads upon the presently claimed trusted module, which is a part of a computer platform and as such implemented in the hardware, software, or both hardware and software of the platform. The passport of Chang is in essence a data file generated by a compiler based upon the original source code, the application writer's private key, and the application writer's license. Applicants do not agree that there are any similarities between these two elements.

Further to the above, Applicants respectfully submit that the present Action does not meet the requirements for a proper 35 USC §103 rejection as set forth in the MPEP as well as the new

KSR v. Teleflex Examination Guidelines of October 10, 2007.

The new Guidelines provide that “When making an obviousness rejection, Office personnel must therefore ensure that the written record includes findings of fact concerning the state of the art and the teachings of the references applied. In certain circumstances, it may also be important to include explicit findings as to how a person of ordinary skill would have understood prior art teachings, or what a person of ordinary skill would have known or could have done. Factual findings made by Office personnel are the necessary underpinnings to establish obviousness.” There are no such factual findings in the present Action, rather in their stead conclusions drawn by the Examiner as to what the skilled person would, in the Examiner’s opinion, have done.

The Guidelines further admonish that “Although a rejection need not be based on a teaching or suggestion to combine, a preferred search will be directed to finding references that provide such a teaching or suggestion if they exist.” The Examiner has cited to Chang’s teaching of a software passport for the purpose of providing the basis of a trust model and allowing computer users to identify and determined the genuineness of a software product based on the information contained in its passport as providing such a suggestion, but Applicants respectfully traverse this reasoning because allowing computer users to identify and determine the genuineness of a software product has absolutely no bearing upon the system of Levy, which is directed to verifying the underlying bytecodes generated by an executing virtual machine. There is absolutely nothing in Levy that would move the skilled reader to be concerned about identifying and determining the genuineness of a software product, as all that Levy is concerned with is the correct compilation of a software product into machine-executable instructions.

The Guidelines further set forth that “Any obviousness rejection should include, either explicitly or implicitly in view of the prior art applied, an indication of the level of ordinary skill.” Applicants have not been able to find such an indication, explicit or implicit, in the Examiner’s Action.

Perhaps the most instructive portion of the Guidelines is the clear statement that “The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in KSR noted that the analysis

supporting a rejection under 35 U.S.C. 103 should be made explicit. The Court quoting In re Kahn stated that “ ‘[R]ejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.’ ” Again, rather than offer articulated reasoning with some rational underpinning, the Examiner merely draws a conclusion of obviousness in light of an assertion of motivation that finds no logical support in the main, Levy reference.

These Guidelines do make clear that “the familiar teaching-suggestion-motivation (TSM) rationale” can still be employed by Examiners in making an obviousness rejection. However, the Examiner has made no mention of where such suggestion is to be found in either of the cited references.

~ ~ ~

Regarding the prior art made of record by the Examiner but not relied upon, Applicants believe that this art does not render the pending claims unpatentable.

In light of all of the above, Applicants respectfully submit that all claims are in fact novel and non-obvious over the art on record and that the application is now in condition for allowance, and respectfully urge the Examiner to pass this case to issue.

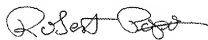
\* \* \*

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025, including the excess independent claim fees due. Furthermore, if this response is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this document is being transmitted to the  
Patent and Trademark Office via electronic filing.

March 31, 2008  
(Date of Transmission)

Respectfully submitted,



Robert Popa  
Attorney for Applicants  
Reg. No. 43,010  
LADAS & PARRY  
5670 Wilshire Boulevard, Suite 2100  
Los Angeles, California 90036  
(323) 934-2300 voice  
(323) 934-0202 facsimile  
rpopa@la.ladas.com